An Achievable Rate Region for the Broadcast Wiretap Channel with Asymmetric Side Information

Maël Le Treust, Abdellatif Zaidi, Samson Lasaulce

An Achievable Rate Region for the Broadcast Wiretap Channel with Asymmetric Side Information

Maël Le Treust*, Abdellatif Zaidi† and Samson Lasaulce*
*Laboratoire des Signaux et Systèmes, CNRS - Université Paris-Sud 11 - Supélec, 91191, Gif-sur-Yvette Cedex, France
Email: {letreust},{lasaulce}@lss.supelec.fr
†Institut Gaspard Monge, Université Paris-Est Marne La Vallée, 77454, Marne La Vallée Cedex 2, France
Email: abdellatif.zaidi@univ-mlv.fr

***Abstract*—The communication scenario under consideration in this paper corresponds to a multiuser channel with side information and consists of a broadcast channel with two legitimate receivers and an eavesdropper. Mainly, the results obtained are as follows. First, an achievable rate region is provided for the (general) case of discrete-input discrete-output channels, generalizing existing results. Second, the obtained theorem is used to derive achievable transmission rates for two practical cases of Gaussian channels. It is shown that known perturbations can enlarge the rate region of broadcast wiretap channels with side information and having side information at the decoder as well can increase the secrecy rate of channels with side information. Third, we establish for the first time an explicit connection between multiuser channels and observation structures in dynamic games. In this respect, we show how to exploit the proved achievability theorem (discrete case) to derive a communication-compatible upper bound on the minmax level of a player.**

I. Introduction

The notion of secrecy in communication systems has been widely studied since 1949 and the publication of [18] by Shannon. He introduced a measure of secrecy for communication systems called equivocation. The secrecy capacity of the general wiretap channel which consists of one transmitter, one legitimate receiver, and one eavesdropper has been determined in [21]. In [6], the authors extended this result assuming that both the legitimate receiver (to which the confidential message is intended) and the eavesdropper have to decode a common message. Regarding broadcast channels, there are at least three other relevant works. The authors of [19] investigate a broadcast channel with side information or state at the encoder. In this model, the transition probability is controlled by a sequence of i.i.d. parameters whose realizations are known non-causally and perfectly by the encoder. They conclude that in the Gaussian case, there is no loss of rate of communication. The authors of [2] provide an achievable rate region for the broadcast channel with two legitimate receivers (each of them having to decode a private and a confidential message) and an eavesdropper; the corresponding region is shown to be tight in the case of physically degraded broadcast channels. For the case of reversely degraded parallel broadcast channels, one eavesdropper, and an arbitrary number of legitimate receivers, the authors of [13] determined the secrecy capacity for transmitting a common message, and the secrecy sum-capacity for transmitting independent messages.

As far as the present work is concerned, the most relevant contribution is provided in [3]. Therein, the authors provide an achievable rate of the discrete or general wiretap channel when a side information is known non-causally to the transmitter (in the sense of [10]). Their achievable secured rate is the minimum between the secure rate of the wiretap channel [21] and the rate of the channel with side information provided by Gel'fand and Pinsker in [10]. The coding scheme in [3] is proved to achieve at least one of these two rates and also satisfy the security constraints $R \leq \frac{H(m|Z^n)}{n}$ where m is the source message, n is the codeword size, and Z^n the observation vector of the eavesdropper.

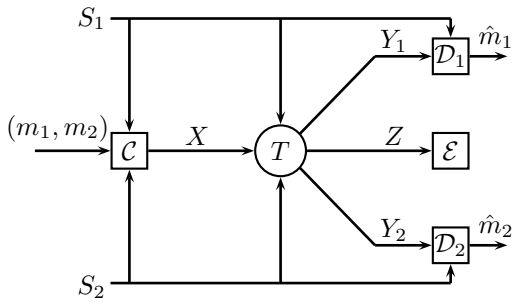

Fig. 1. The broadcast wiretap channel with asymmetric side information. The encoder $\mathcal{C}$ send the message m_1 (resp. m_2) to decoder $\mathcal{D}_1$ (resp. $\mathcal{D}_2$) through the channel T by preventing the eavesdropper $\mathcal{E}$ to decode. X is the channel input, S_1 and Y_1 (resp. S_2 and Y_2) are the side information and the channel output available at the first (resp. second) decoder, Z is the channel output for the eavesdropper.

We extend this result by considering the broadcast channel with confidential messages represented in Fig. 1. With respect to [3], two differences have to be noticed.

- A two-user broadcast channel is considered.
- Each legitimate receiver only knows a part of the side information.

To be more precise, if (S_1, S_2) represents the pair of side information, receiver or decoder $\mathcal{D}_k$, with $k \in \{1, 2\}$, knows only S_k. On the other hand, the eavesdropper $\mathcal{E}$ does not know the side information at all.

The two main motivations for deriving an achievable rate region for this multiuser channel are as follows. First of all, the goal is to better understand the influence of the side

information on the performance limits of secure communications. The second strong motivation is more original since we show that coding theorems are also useful for understanding strategic interactions (games). Indeed, as mentioned in [14], there has been, in recent years, a surge of interest for game theory since it can be useful to analyze multiuser settings (the interference channel is one of them [20], [9]). In those studies, quite often, Shannon transmission rates are considered for the player's utilities and game-theoretic notions are applied. One of the messages of the present work is that, conversely, multiuser channels can be used to understand (dynamic) games with arbitrary observation structures and utility functions. This contributes to strengthen the links between Shannon theory and game theory and gives more momentum to some works in this direction such as [1] [16].

In the next section II, we introduce the channel model under investigation and the main achievability result (Theorem 4). We compare the derived result with previous works in Sec. III. In Sec. IV, we prove theorem 4. Sec. V is devoted to exploiting the derived theorem in the Gaussian case (achievability theorems follow in the Gaussian case provided long but simple calculations are done, the latter are omitted here). We consider, in Sec. VI, a direct application of our result to games. We provide an upper bound on the min-max level in a four-player long-run game with a given observation/monitoring structure (called games with signals in the literature of game theory). We conclude the paper by summarizing remarks and possible extensions of this work (Sec. VII).

II. Channel model

In this paper, we denote X, S_1, S_2, Y_1, Y_2, Z the random variables of the channel inputs $x \in \mathcal{X}$, the side information at the first $s_1 \in \mathcal{S}_1$ and the second $s_2 \in \mathcal{S}_2$ decoders, the channel ouputs for the first $y_1 \in \mathcal{Y}_1$ and the second $y_2 \in \mathcal{Y}_2$ decoders and the channel ouputs $z \in \mathcal{Z}$ for the eavesdropper (see Fig 1). The corresponding sequences will be written $Z^n = (Z(1), \ldots, Z(n))$, where superscripted letters denote the vector. The messages m_1 and m_2 are uniformly distributed among the sets $\mathcal{M}_1$ and $\mathcal{M}_2$ whose cardinalities are denoted $M_1 = |\mathcal{M}_1|$ and $M_2 = |\mathcal{M}_2|$. $\Delta(\mathcal{Y})$ denote the set of probability distributions over the set $\mathcal{Y}$, $\mathcal{P}^{\otimes n} \in \Delta(\mathcal{X}^n)$ denote the n-times product of the probability $\mathcal{P} \in \Delta(\mathcal{X})$ and co $\mathcal{R}$ denote the convex hull of a set $\mathcal{R}$.

Consider a broadcast wiretap channel with asymmetric side information, as a transition probability described in figure 1

$$T : \mathcal{X} \times \mathcal{S}_1 \times \mathcal{S}_2 \longrightarrow \Delta(\mathcal{Y}_1 \times \mathcal{Y}_2 \times \mathcal{Z}). \tag{1}$$

The side information s_1, s_2 are drawn independently and identically distributed from the joint distribution $P_s \in \Delta(\mathcal{S}_1 \times \mathcal{S}_2)$. The sequence of realizations s_1^n, s_2^n are non-causally known at the encoder and at their respective decoders. The channel is discrete and memoryless, i.e. the n-stage transition probability is defined as follows:

$$\begin{aligned} &T^{\otimes n}(y_1^n, y_2^n, z^n | x^n, s_1^n, s_2^n) \\ &= \prod_{i=1}^{n} T(y_1(i), y_2(i), z(i) | x(i), s_1(i), s_2(i)). \end{aligned} \tag{2}$$

Definition 1: Define an (n, M_1, M_2)-code as a triplet of functions as follows:

$$f \quad : \mathcal{M}_1 \times \mathcal{M}_2 \times \mathcal{S}_1^n \times \mathcal{S}_2^n \longrightarrow \mathcal{X}^n, \tag{3}$$

$$g_1 \quad : \mathcal{Y}_1^n \times \mathcal{S}_1^n \longrightarrow \mathcal{M}_1, \tag{4}$$

$$g_2 \quad : \mathcal{Y}_2^n \times \mathcal{S}_2^n \longrightarrow \mathcal{M}_2. \tag{5}$$

$(\hat{m}_1, \hat{m}_2)$ denote the random variable of the messages reconstructed by the code. Define the error probability $\mathcal{P}_e^n$ associated with each (n, M_1, M_2)-code as follows:

$$\mathcal{P}_e^n = \mathcal{P}((m_1, m_2) \neq (\hat{m}_1, \hat{m}_2)). \tag{6}$$

The amount of information of a code is related to the cardinality M_1 and M_2 of the sets of messages $\mathcal{M}_1$ and $\mathcal{M}_2$. As in [17], this quantity is measured by the rate $R = \frac{\log M}{n}$ of the code. In the context of secure communication, the notion of equivocation $\frac{H(m|Z^n)}{n}$ [18] is introduced as a measure of the secrecy level guaranteed by a code. When this level is greater than the rate of the code, it prevents the eavesdropper from correctly decoding the transmitted information.

Definition 2: A rate pair (R_1, R_2) is said to be achievable if for all $\varepsilon > 0$, there exists a (n, M_1, M_2)-code such that:

$$\frac{\log M_1}{n} \geq R_1 - \varepsilon, \tag{7}$$

$$\frac{\log M_2}{n} \geq R_2 - \varepsilon, \tag{8}$$

$$\frac{H(m_1|Z^n)}{n} \geq R_1 - \varepsilon, \tag{9}$$

$$\frac{H(m_2|Z^n)}{n} \geq R_2 - \varepsilon, \tag{10}$$

$$\frac{H(m_1, m_2|Z^n)}{n} \geq R_1 + R_2 - \varepsilon, \tag{11}$$

$$\mathcal{P}_e^n \leq \varepsilon. \tag{12}$$

Denote $\mathcal{R}$ the set of achievable rate pairs.

A. Main result

We provide an achievable rate region for the considered broadcast wiretap channel with asymmetric side information.

Definition 3: Denote $\mathcal{R}_I$ the set of rate pairs (R_1, R_2) such that there exists a probability distribution $\mathcal{P}(u_1, u_2, x | s_1, s_2)$ satisfying:

$$\begin{aligned} R_1 &\leq I(U_1; Y_1, S_1) - \max(I(U_1; Z), I(U_1; S_1, S_2)), \\ R_2 &\leq I(U_2; Y_2, S_2) - \max(I(U_2; Z), I(U_2; S_1, S_2)), \\ R_1 + R_2 &\leq I(U_1; Y_1, S_1) + I(U_2; Y_2, S_2) - I(U_1; U_2) \\ &\quad - \max(I(U_1, U_2; Z), I(U_1, U_2; S_1, S_2)). \end{aligned} \tag{13}$$

Remark that the probability $\mathcal{P}(u_1, u_2, x | s_1, s_2)$ induces a general distribution $\mathcal{Q}$ that satisfies the Markov property $(U_1, U_2) - (X, S_1, S_2) - (Y_1, Y_2, Z)$. This probability $\mathcal{Q}$ is

defined for every $(u_1, u_2, x, s_1, s_2, y_1, y_2, z)$, by the following equation:

$$\mathcal{Q}(u_1, u_2, x, s_1, s_2, y_1, y_2, z) = P_s(s_1, s_2) \times \mathcal{P}(u_1, u_2, x|s_1, s_2) \times T(y_1, y_2, z|x, s_1, s_2).$$

Theorem 4: Any rate pair $(R_1, R_2) \in$ co $\mathcal{R}_I$ is achievable for the broadcast wiretap channel with asymmetric side information.

Suppose that we need the channel input to be correlated with a sequence of i.i.d. random variable S^n. The analysis leads to consider the random variable S as a side information even if it does not impact the transition probability. This remark applies, more specifically, in a game theoretical framework (see Sec. VI).

III. Interpretation

The achievable rate region $\mathcal{R}_I$ we provide is a generalization of the one in [3]. It consists in the intersection of two rate regions. The first one is related to the side information as in [19] and the second one is related to the eavesdropper as in [2]. Note that if we remove the eavesdropper ($Z = \mathcal{C}$) and we consider that the side information is non-causally known only at the encoder, our rate region boils down to the one of [19] when the variable W is constant. If we remove the side information ($S_1 = S_2 = \mathcal{C}$), the rate region equals the one described in [2]. Suppose we remove the receivers ($\mathcal{D}_2$) and the side information ($S_1 = \mathcal{C}$) and in that case the rate region boils down to the one of the article [3].

IV. Proof of theorem 4

We first prove the achievability of the rate pair $(R_1, R_2) \in \mathcal{T}_I$ satisfying the above inequalities (13). Fix a distribution $\mathcal{Q}(u_1, u_2, x, s_1, s_2, y_1, y_2, z)$ satisfying the channel transition $T(y_1, y_2, z|x, s_1, s_2)$, the distribution $P_s(s_1, s_2)$ and the rates inequalities (13). We will prove that the pair $(R_1, R_2) \in \mathcal{T}_I$ is achievable. Denote $A_\varepsilon^{*n}(U_1 \times U_2|s_1^n, s_2^n)$ the set of sequences u_1^n, u_2^n that are jointly typical with s_1^n, s_2^n. The properties of the typical sequences can be founded in [5] and [7].

- Generation of the Code-book : Generate $M_{Y_1} = 2^{nR_{Y_1}} = 2^{n(I(U_1;Y_1,S_1)-\varepsilon)}$ sequences u_1^n from distribution $\mathcal{Q}_{U_1}(u_1)^{\otimes n}$. Distribute them at random into $M_1 = 2^{nR_1}$ bins denoted $i_1 \in \{1, \ldots, M_1\}$, containing each of them $M_{U_1} = 2^{nR_{U_1}}$ sequences u_1^n. Divide each bin i_1 into $M_{W_1} = 2^{nR_{W_1}}$ sub-bins denoted $j_1 \in \{1, \ldots, M_{W_1}\}$ containing each of them $M_{Z_1} = 2^{nR_{Z_1}}$ sequences u_1^n with the following parameters $R_{U_1}, R_{Y_1}, R_1, R_{Z_1}$. Generate $M_{Y_2} = 2^{nR_{Y_2}} = 2^{n(I(U_2;Y_2,S_2)-\varepsilon)}$ sequences u_2^n from distribution $\mathcal{Q}_{U_2}(u_2)^{\otimes n}$. Distribute them at random into $M_2 = 2^{nR_2}$ bins denoted $i_2 \in \{1, \ldots, M_2\}$, containing each of them $M_{U_2} = 2^{nR_{U_2}}$ sequences u_2^n. Divide each bin i_2 into $M_{W_2} = 2^{nR_{W_2}}$ sub-bins denoted $j_2 \in \{1, \ldots, M_{W_2}\}$ containing each of them $M_{Z_2} = 2^{nR_{Z_2}}$ sequences u_2^n with the above parameters $R_{U_2}, R_{Y_2}, R_2, R_{Z_2}$. For each tuple of sequences $(u_1^n, u_2^n, s_1^n, s_2^n)$ draw a sequence x^n from the distribution $\mathcal{Q}(x|u_1, u_2, s_1, s_2)^{\otimes n}$.
- Encoder obtains the message $(i_1, i_2) \in \mathcal{M}_1 \times \mathcal{M}_2$ and the sequence of side information (s_1^n, s_2^n). It finds a pair of sequences u_1^n in the bin i_1 and u_2^n in the bin i_2 such that $(u_1^n, u_2^n) \in A_\varepsilon^{*n}(U_1 \times U_2|s_1^n, s_2^n)$. Send the sequence x^n corresponding to the tuple of sequences $(u_1^n, u_2^n, s_1^n, s_2^n)$.

$$\begin{aligned} R_{U_1} &> I(U_1; S_2, S_1), \\ R_{U_2} &> I(U_2; S_1, S_2), \\ R_{U_1} + R_{U_2} &> I(U_1; U_2) + I(U_1, U_2; S_1, S_2), \end{aligned}$$

$$\begin{aligned} R_{Y_1} = R_{U_1} + R_1 &< I(U_1; Y_1, S_1), \\ R_{Y_2} = R_{U_2} + R_1 &< I(U_2; Y_2, S_2), \end{aligned}$$

$$\begin{aligned} R_{Z_1} &< I(U_1; Z), \\ R_{Z_2} &< I(U_2; Z), \\ R_{Z_1} + R_{Z_2} &< I(U_1; U_2) + I(U_1, U_2; Z), \end{aligned}$$

$$\begin{aligned} R_{U_1} &> R_{Z_1}, \\ R_{U_2} &> R_{Z_2}. \end{aligned}$$

- Decoder 1 receives the channel output y_1^n and the sequence of side information s_1^n. It finds a unique sequence u_1^n such that $u_1^n \in A_\varepsilon^{*n}(U_1|y_1^n, s_1^n)$ and it returns the bin index i_1 of the sequence u_1^n.
- Decoder 2 receives the channel output y_2^n and the sequence of side information s_2^n. It finds a unique sequence u_2^n such that $u_2^n \in A_\varepsilon^{*n}(U_2|y_2^n, s_2^n)$ and it returns the bin index i_2 of the sequence u_2^n.

The proof consists first to show that the error probability can be upper bounded by $\varepsilon > 0$ as n goes to infinity. Second, we check if the equivocation rate at the eavesdropper is sufficiently high as n goes to infinity. We conclude that the desired rate (R_1, R_2) pair belongs to the achievable rate region that satisfies by the above inequalities (13).

Analysis of the error probability. As in the articles [10] and [15], it is based on extensions of the following lemma:

Lemma 1: The properties of the typical sequences [7]. Let the joint probability $\mathcal{Q}(x, y) \in \Delta(X \times Y)$, then:

$$\mathcal{Q}^{\otimes n}(x^n \in A_\varepsilon^{n*}(X|y^n)|y^n) \geq 1 - \varepsilon \qquad \forall y^n \in A_\varepsilon^{n*}(Y).$$

Lemma 2: The mutual covering lemma [8]. Suppose that the family of sequences $(u(i)^n)_{i \in 2^{nR_I}} \in U^n$ is drawn i.i.d. from $\mathcal{Q}_U^{\otimes n}$ and $(v(j)^n)_{j \in 2^{nR_J}}$ is drawn i.i.d. from $\mathcal{Q}_V^{\otimes n}$. Then for all $\varepsilon > 0$, there exists an $\bar{n} \geq 0$ such that for all $n \geq \bar{n}$:

$$\begin{aligned} &R_I + R_J < I(U; V) \Longrightarrow \\ &\mathcal{P}(\cup_{\substack{i \in I, \\ j \in J}} \{(u(i)^n, v(j)^n) \in A_\varepsilon^{*n}(U \times V)\}) \leq \varepsilon, \\ &R_I + R_J > I(U; V) \Longrightarrow \\ &\mathcal{P}(\cap_{\substack{i \in I, \\ j \in J}} \{(u(i)^n, v(j)^n) \notin A_\varepsilon^{*n}(U \times V)\}) \leq \varepsilon. \end{aligned}$$

Without loss of generality, we assume that the encoder has to transmit the messages (i_1, i_2). Denote B_{i_1} and B_{i_2} the bins of

sequences u_1^n and u_2^n respectively. Let us define the following error events:

- $\mathcal{E}_1 = \{(s_1^n, s_2^n) \notin A_\varepsilon^{*n}(S_1 \times S_2)\}$ the two sequences of side information are not jointly typical.
- $\mathcal{E}_2 = \{\forall (u_1^n, u_2^n) \in B_{i_1} \times B_{i_2},\ (u_1^n, u_2^n) \notin A_\varepsilon^{*n}(U_1 \times U_2 | s_1^n, s_2^n)\}$ there is no pair of sequence (u_1^n, u_2^n) in the bins B_{i_1} and B_{i_2} that are jointly typical with (s_1^n, s_2^n).
- $\mathcal{E}_3 = \{(x^n, y_1^n, y_2^n, z^n) \notin A_\varepsilon^{*n}(X \times Y_1 \times Y_2 \times Z | u_1^n, u_2^n, s_1^n, s_2^n) | (u_1^n, u_2^n, s_1^n, s_2^n) \in A_\varepsilon^{*n}(U_1 \times U_2 \times S_1 \times S_2\}$ the family (x^n, y_1^n, y_2^n, z^n) of sequences is not jointly typical with the jointly typical sequences $(u_1^n, u_2^n, s_1^n, s_2^n)$.
- $\mathcal{E}_4 = \{\exists u_1^{'n} \neq u_1^n,\ (u_1^{'n}, y_1^n, s_1^n)^n \in A_\varepsilon^{*n}(U_1 \times Y_1 \times S_1)\}$ there is another vector $u_1^{'n}$ jointly typical with the channel output y_1^n and the side information s_1^n.
- $\mathcal{E}_5 = \{\exists u_2^{'n} \neq u_2^n,\ (u_2^{'n}, y_2^n, s_2^n) \in A_\varepsilon^{*n}(U_2 \times Y_2 \times S_2)\}$ there is another vector $u_2^{'n}$ jointly typical with the channel output y_2^n and the side information s_2^n.

Using an extension of covering lemma [8], we bound $\mathcal{P}(\mathcal{E}_2)$ by ε as soon as, the following inequalities are satisfied.

$$\begin{aligned} R_{U_1} &> I(U_1; S_2, S_1), && (14)\\ R_{U_2} &> I(U_2; S_1, S_2), && (15)\\ R_{U_1} + R_{U_2} &> I(U_1; U_2) + I(U_1, U_2; S_1, S_2). && (16) \end{aligned}$$

$\mathcal{P}(\mathcal{E}_4)$ and $\mathcal{P}(\mathcal{E}_5)$ are bounded by ε if:

$$\begin{aligned} R_{Y_1} = R_{U_1} + R_1 &< I(U_1; Y_1, S_1), && (17)\\ R_{Y_2} = R_{U_2} + R_1 &< I(U_2; Y_2, S_2). && (18) \end{aligned}$$

To bound $\mathcal{P}(\mathcal{E}_1)$ and $\mathcal{P}(\mathcal{E}_3)$, we use classical properties of the typical sequences [7]. Thus for all ε, there exists n such that,

$$\mathcal{P}_e^n \leq 5\varepsilon. \quad (19)$$

We proved that the error probability is upper bounded by 5ε.

The equivocation rate at the eavesdropper.
Denote (m_1, m_2) the random variable of the pair of bins and (w_1, w_2) the random variable of the pair of sub-bins. Let us prove that $\frac{H(m_1,m_2|Z^n)}{n} \geq R_1 + R_2 - \varepsilon$. We first introduce the random variables w_1, w_2 and U_1^n, U_2^n in the expression of $H(m_1, m_2|Z^n)$.

$$\begin{aligned} & H(m_1, m_2|Z^n)\\ =\ & H(m_1, m_2, Z^n) - H(Z^n)\\ =\ & H(m_1, m_2, w_1, w_2, Z^n)\\ & -H(w_1, w_2|m_1, m_2, Z^n) - H(Z^n)\\ =\ & H(m_1, m_2, w_1, w_2, U_1^n, U_2^n, Z^n)\\ & -H(U_1^n, U_2^n|m_1, m_2, w_1, w_2, Z^n)\\ & -H(w_1, w_2|m_1, m_2, Z^n) - H(Z^n) \end{aligned} \quad (20)$$

$$\begin{aligned} =\ & H(m_1, m_2, w_1, w_2|U_1^n, U_2^n, Z^n)\\ & +H(U_1^n, U_2^n, Z^n)\\ & -H(U_1^n, U_2^n|m_1, m_2, w_1, w_2, Z^n)\\ & -H(w_1, w_2|m_1, m_2, Z^n) - H(Z^n)\\ =\ & H(m_1, m_2, w_1, w_2|U_1^n, U_2^n, Z^n) && (21)\\ & +H(U_1^n, U_2^n|Z^n) && (22)\\ & -H(U_1^n, U_2^n|m_1, m_2, w_1, w_2, Z^n) && (23)\\ & -H(w_1, w_2|m_1, m_2, Z^n). && (24) \end{aligned}$$

We provide a lower bound for each of the four terms of the above equation.
The first term (21) in the above equation is removed.
The second term (22) is lower bounded, using the chain rule [5], by the following quantity:

$$\begin{aligned} & H(U_1^n, U_2^n|Z^n)\\ =\ & H(U_1^n) + H(U_2^n) - I(U_1^n; U_2^n) - I(U_1^n, U_2^n; Z)\\ \geq\ & I(U_1^n; Y_1^n, S_1^n) + I(U_2^n; Y_2^n, S_2^n)\\ & -I(U_1^n; U_2^n) - I(U_1^n, U_2^n; Z)\\ \geq\ & n[I(U_1; Y_1, S_1) + I(U_2; Y_2, S_2)\\ & -I(U_1; U_2) - I(U_1, U_2; Z)]. \end{aligned}$$

The third term (23) is lower bounded by $-2\varepsilon - n2\varepsilon \log|Z|$ using Fano's inequality [5] and the following system of conditions:

$$\begin{aligned} R_{Z_1} &< I(U_1; Z), && (25)\\ R_{Z_2} &< I(U_2; Z), && (26)\\ R_{Z_1} + R_{Z_2} &< I(U_1; U_2) + I(U_1, U_2; Z). && (27) \end{aligned}$$

Denote B_{m_1} the bin with index m_1 and B_{w_1} the sub-bin with index w_1. Let the following events:

$$\begin{aligned} \mathcal{E}_6 =\ & \{\forall (u_1, u_2) \in (B_{m_1} \times B_{m_2}) \cap (B_{w_1} \times B_{w_2}),\\ & (u_1^n, u_2^n, z^n) \notin A_\varepsilon^{*n}(U_1 \times U_2 \times Z)\},\\ \mathcal{E}_7 =\ & \{\exists (u_1, u_2)' \neq (u_1, u_2)\\ & \in (B_{m_1} \times B_{m_2}) \cap (B_{w_1} \times B_{w_2}),\\ & s.t. (u_1', u_2', z) \in A_\varepsilon^{*n}(U_1 \times U_2 \times Z)\}. \end{aligned}$$

Consider a typical decoding function of the eavesdropper knowing the pairs of bin indexes (m_1, m_2) and sub-bin index (w_1, w_2),

$$g : \mathcal{Z}^n \longrightarrow \mathcal{U}_1^n \times \mathcal{U}_2^n. \quad (28)$$

To the received sequence z^n, it associates the pair (u_1^n, u_2^n) if it belong to the bins (m_1, m_2), the sub-bins (w_1, w_2) and is jointly typical with z^n. Define the error probability of such a decoding function

$$\begin{aligned} \mathcal{P}_{æ} =\ & \mathcal{P}((U_1^n, U_2^n) \neq g(Z^n) \text{ s.t. } (U_1^n, U_2^n) \in\\ & (B_{m_1} \times B_{m_2}) \cap (B_{w_1} \times B_{w_2})) && (29)\\ \leq\ & \mathcal{P}(\mathcal{E}_6) + \mathcal{P}(\mathcal{E}_7) \leq 2\varepsilon, && (30) \end{aligned}$$

where $\mathcal{P}(\mathcal{E}_6) \leq \varepsilon$ comes from properties of the typical sequences [7] and $\mathcal{P}(\mathcal{E}_7) \leq \varepsilon$ comes from the above system of equations (25)-(27). Using Fano's inequality [5] we have:

$$\begin{aligned} & H(U_1^n, U_2^n | m_1, m_2, w_1, w_2, Z^n) \\ \leq\ & H(\mathcal{P}_{æ}) + n\mathcal{P}_{æ}(\log|Z| - \varepsilon) \\ \leq\ & 2\varepsilon + n2\varepsilon \log|Z|. \end{aligned}$$

The fourth term (24) is lower bounded by the following quantity: $-n(\max[I(U_1, U_2; S_1, S_2) - I(U_1, U_2; Z), 0] + 4\varepsilon)$. From the condition (16) and the definition of the sub-bins we have:

$$\begin{aligned} R_{U_1} + R_{U_2} \quad \geq \quad & \max[I(U_1, U_2; S_1, S_2) \\ & + I(U_1; U_2), R_{Z_1} + R_{Z_2}]. \end{aligned} \tag{31}$$

Suppose that the two following conditions are satisfied:

$$\begin{aligned} R_{U_1} + R_{U_2} \quad \leq \quad & \max[I(U_1, U_2; S_1, S_2) \\ & + I(U_1; U_2), R_{Z_1} + R_{Z_2}] + 2\varepsilon, \end{aligned} \tag{32}$$

$$R_{Z_1} + R_{Z_2} \quad \geq \quad I(U_1; U_2) + I(U_1, U_2; Z) - 2\varepsilon. \tag{33}$$

We now prove the following inequalities:

$$\begin{aligned} & H(w_1, w_2 | m_1, m_2, Z^n) \\ \leq\ & \log(|W_1| \times |W_2|) \\ =\ & n(R_{U_1} + R_{U_2} - R_{Z_1} - R_{Z_2}) \\ \leq\ & n(\max[I(U_1; U_2) + I(U_1, U_2; S_1, S_2), \\ & I(U_1; U_2) I(U_1, U_2; Z)] + 2\varepsilon \\ & - I(U_1; U_2) - I(U_1, U_2; Z) + 2\varepsilon) \\ \leq\ & n(\max[I(U_1, U_2; S_1, S_2) - I(U_1, U_2; Z), 0] + 4\varepsilon). \end{aligned}$$

Combining the four above terms, we obtain the lower bound $R_1 + R_2 - \bar{\varepsilon}$ over the equivocation rate.

$$\begin{aligned} & H(m_1, m_2 | Z^n) \\ \geq\ & n(I(U_1; Y_1, S_1) + I(U_2; Y_2, S_2) \\ & - I(U_1; U_2) - I(U_1, U_2; Z)) - 2\varepsilon - n2\varepsilon \log|Z| \\ & - n(\max(I(U_1, U_2; S_1, S_2) - I(U_1, U_2; Z), 0) + 4\varepsilon) \\ \geq\ & n(I(U_1; Y_1, S_1) + I(U_2; Y_2, S_2) \\ & - I(U_1; U_2) - \max(I(U_1, U_2; S_1, S_2), I(U_1, U_2; Z))) \\ & - 2\varepsilon - n\varepsilon(2\log|Z| + 4) \\ \geq\ & n(R_1 + R_2) - 2\varepsilon - n\varepsilon(2\log|Z| + 4). \end{aligned}$$

$$\iff \frac{I(m_1, m_2; Z^n)}{n} \quad \leq \quad \bar{\varepsilon}.$$

With $\bar{\varepsilon} = \varepsilon(2/n + 2\log|Z| + 4)$. The same arguments apply to prove that:

$$\frac{H(m_1|Z^n)}{n} \geq R_1 - \bar{\varepsilon}, \tag{34}$$

$$\frac{H(m_2|Z^n)}{n} \geq R_2 - \bar{\varepsilon}. \tag{35}$$

The transmission rates are determined by the binning scheme:

$$\begin{aligned} R_1 \quad &= \quad R_{Y_1} - R_{U_1}, \\ R_2 \quad &= \quad R_{Y_2} - R_{U_2}, \\ R_1 + R_2 \quad &= \quad (R_{Y_1} + R_{Y_2}) - R_{U_1} - R_{U_2}. \end{aligned}$$

We have proven that our coding scheme achieves every rate pair of the following rate region $\mathcal{R}_I$.

$$\begin{aligned} R_1 \quad &\leq \quad I(U_1; Y_1, S_1) - \max[I(U_1; Z), I(U_1; S_1, S_2)], \\ R_2 \quad &\leq \quad I(U_2; Y_2, S_2) - \max[I(U_2; Z), I(U_2; S_1, S_2)], \\ R_1 + R_2 \quad &\leq \quad I(U_1; Y_1, S_1) + I(U_2; Y_2, S_2) - I(U_1; U_2) \\ & - \quad \max[I(U_1, U_2; Z); I(U_1, U_2; S_1, S_2)]. \end{aligned}$$

A classical time-sharing argument in the coding scheme implies that the convex hull $\text{co}\,\mathcal{R}_I$ of the rate region is achievable.

V. The case of Gaussian channels

In this section, we want to show theorem 4 can be exploited for Gaussian communication channels. At least two interesting results are emphasized. For the first model under consideration (Fig. 2), it is shown that the presence of known perturbations (namely S_1 and S_2) can enhance the secrecy rates. In fact, if those perturbations are sufficiently strong, it is even possible to obtain the same rate region as if the eavesdropper were not present. For the second model (Fig. 4), it is shown that knowing the side information can lead to a larger secrecy rate, which is usually not the case in channels with states but with no eavesdropper.

A. Increasing the influence of known perturbations enhances the rate region

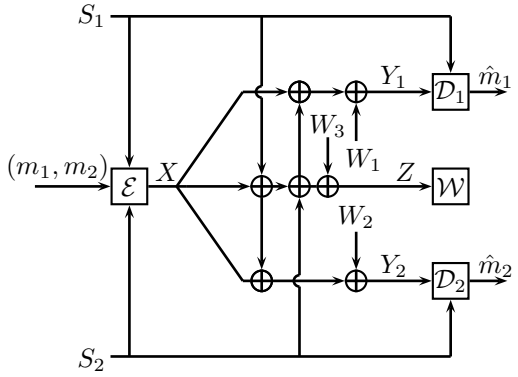

Fig. 2. The Gaussian broadcast wiretap channel with asymmetric side information.

The Gaussian broadcast wiretap channel with asymmetric side information we consider is described by the following equations:

$$Y_1 \quad = \quad X + S_2 + W_1 \tag{36}$$

$$Y_2 \quad = \quad X + S_1 + W_2 \tag{37}$$

$$Z \quad = \quad X + S_1 + S_2 + W_3 \tag{38}$$

The random variables W_1, W_2, W_3, S_1, S_2 are Gaussian with mean 0 and variance N_1, N_2, N_3, Q_1, Q_2. The channel states S_1 and S_2 are correlated following the parameter $\rho = \frac{\mathbb{E}[S_1 S_2]}{\sqrt{Q_1 Q_2}}$. The channel input X must satisfy the constraint:

$$\mathbb{E}[X^2] \leq P \tag{39}$$

Without loss of generality, we suppose that $N_1 \geq N_2$. The channel of the first receiver is physically degradable version of the second one. Let $\alpha_1 \in \mathbb{R}, \alpha_2 \in \mathbb{R}, \beta \in [0,1]$ and $\bar{\beta} = 1-\beta$. Decompose $X = X_1 + X_2$ into two independent Gaussian random variables X_1 and X_2 with mean 0 and variance βP and $\bar{\beta} P$. Define the following auxiliary random variables:

$$\begin{aligned} U_1 = X_1 + \alpha_1 S_2 &\sim \mathcal{N}(0, \beta P + \alpha_1^2 Q_2) \\ U_2 = X_2 + \alpha_2 (S_1 + X_1) &\sim \mathcal{N}(0, \bar{\beta} P + \alpha_2^2 (Q_1 + \beta P)) \end{aligned}$$

Numerical simulations (Fig. 3) illustrate the achievable rate region comparing to the previous results in [19], [2] and [3]. In Fig. 3, we compare the achievable rate region for different values Q_1 and Q_2 of the variance of the side information S_1, S_2 and for the correlation parameter $\rho = 0$. When the variance of the side information is low $(Q_1 = Q_2 = 0.1)$, the rate region (in blue) is close to the one of [2]. Whereas for high variance of the side information $(Q_1 = Q_2 = 20)$, the rate region (in yellow) is close to the capacity region for the broadcast channel of [19]. High variances Q_1 and Q_2 for the side information are sufficient to compensate for the presence of an eavesdropper in the network.

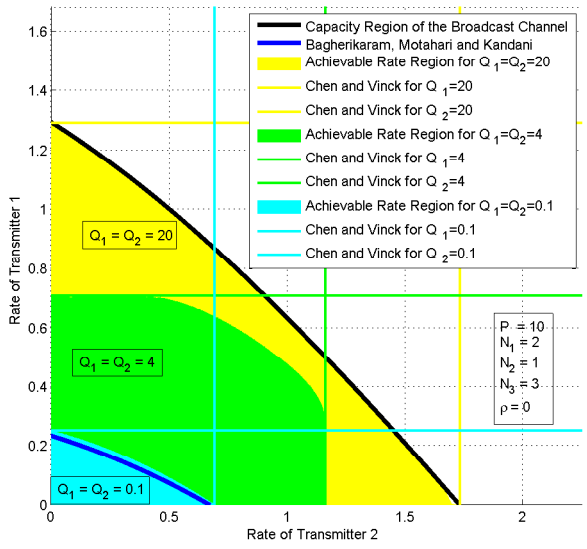

Fig. 3. Rate region for the correlation parameter $\rho = 0$ and different values of Q_1 and Q_2.

B. Having the side information at the decoder as well allows to enlarge the secrecy rate

Often, when already available at the encoder, the knowledge of the side information at the decoder does not increase the transmission rate [4][19]. However, this is not true when considering channels with security constraints. We provide a special case of our channel model for which the knowledge of the side information at the decoder strictly increases the achievable rate.

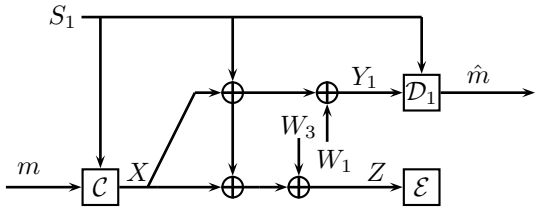

Fig. 4. The Gaussian wiretap channel with side information non-causally known at both the encoder and the decoder.

The Gaussian broadcast wiretap channel with side information at the decoder is described by the following equations:

$$Y_1 = X + S_1 + W_1, \tag{40}$$
$$Z = X + S_1 + W_3. \tag{41}$$

This channel is a special case of the model we consider here above when we remove the decoder $\mathcal{D}_2$ and we fix the second side information constant $\mathcal{S}_2 = \emptyset$. The side information S_1 is non-causally known at the decoder. The random variables W_1, W_3, S_1, are gaussian with mean 0 and variance N_1, N_3, Q_1. The channel input X must satisfies the constraint:

$$\mathbb{E}[X^2] \leq P \tag{42}$$

Theorem 5: The capacity of the channel with state is achievable.

$$\mathcal{C} = I(U_1; Y_1 | S_1).$$

The proof consists in replacing the random variable U_1 with a parameter $\alpha_1 \gg 1$ in the first equation of (13).

VI. Min-max level for a long-run game with signals

The above-referenced channel is now used to model the transmission of strategic information in a long-run game with signals that is, a game where a given player has a certain observation of the actions played by the others [1]. Therefore, in dynamic games with imperfect monitoring/observation, players observe the actions taken by other players through channels also called "signalling structure". An important challenge is to characterize the set of equilibrium utilities for a long-run game with imperfect monitoring; even in the case of repeated games, the problem of finding this set is still open [16]. This problem is closely related to the characterization of achievable rate regions for a class of channel models containing the one we investigate in this paper. Coding/decoding schemes designed for channels with security constraints can allow a group of players to correlate their sequence of plays keeping it secret from another group of players. Our main contribution is to point out a general methodology which can be used in many other scenarios and provide, for a specific example an upper

bound on min-max levels. The example chosen is a four-player repeated game with signals, directly establishing a link with the multiuser channel studied in Sec. II.

A. A repeated game with signals

A stage game is defined by a set of players $\mathcal{K}$, each of them having a set of actions $\mathcal{A}_k$ and a stage-utility function u_k. In a long run game, a strategy $\tau_k = (\tau_k^t)_{1\leq t}$ of player $k \in \mathcal{K}$ is a sequence of functions from the sequences of signals $S_k^{\times(t-1)}$ into the mixed actions $\Delta(\mathcal{A}_k)$:

$$\tau_k^t : \mathcal{S}_k^{\times(t-1)} \quad \longrightarrow \quad \Delta(\mathcal{A}_k) \tag{43}$$

A profile of strategies $\tau = (\tau_k)_{i\in\mathcal{K}}$ induces a probability distribution $\mathcal{P}_\tau \in \Delta(\mathcal{A}^\infty)$ over the sequences of actions $(a^t)_{t\geq 1}$. The utility of the n-stage game is related to the above probability $\mathcal{P}_\tau$.

$$\gamma_k^n(\tau) \quad = \quad \mathbb{E}_\tau \frac{1}{n}\sum_{t=1}^{n} u_k(a_1^t, \ldots, a_K^t) \tag{44}$$

The reader is referred to the paper of Renault and Tomala [16] for more details about the model of repeated games with signals.

B. The min-max levels as "punishment levels"

The min-max level, also called "the punishment level", of a player measures the worst utility level this player can be forced by the others in a long-run game. The formal problem of the min-max levels is in the articles of Gossner and Tomala [11], [12]. They provide a characterization of the min-max using entropy methods. Denote τ_{-k} the vector of strategy of all the players $\ell \neq k \in \mathcal{K}$ except $k \in \mathcal{K}$.

Definition 6: The uniform min-max v_k^∞ for player $k \in \mathcal{K}$ is defined as follows:

- *The players $\ell \neq k \in \mathcal{K}$ guarantee $v_k^\infty \in R$ if:*

$$\forall \varepsilon > 0, \exists \tau_{-k}, \exists N \in \mathbb{N}, \forall \tau_k, \forall n \geq N \tag{45}$$
$$\gamma_k^n(\tau_k, \tau_{-k}) \leq v_k^\infty + \varepsilon \tag{46}$$

- *The player $k \in \mathcal{K}$ defends $v_k^\infty \in R$ if:*

$$\forall \varepsilon > 0, \forall \tau_{-k}, \exists \tau_k, \exists N \in \mathbb{N}, \forall n \geq N \tag{47}$$
$$\gamma_k^n(\tau_k, \tau_{-k}) \geq v_k^\infty - \varepsilon \tag{48}$$

- *The uniform min-max of player $k \in \mathcal{K}$, if it exists, is $v_k^\infty \in \mathbb{R}$ such that players $\ell \neq k \in \mathcal{K}$ guarantee $v_k^\infty \in R$ and player $k \in \mathcal{K}$ defends $v_k^\infty \in R$.*

C. Upper bound on min-max levels

We denote $\mathcal{A}_{123} = \mathcal{A}_1 \times \mathcal{A}_2 \times \mathcal{A}_3$ the product of actions set and $X_{123} = \prod_{k=1,2,3} \Delta(\mathcal{A}_k)$ the product of independent probabilities over the player's actions.

Definition 7: Define $\mathbb{Q}_1 \subset \Delta(\mathcal{A}_1 \times \mathcal{A}_2 \times \mathcal{A}_3)$ the set of achievable empirical distributions, where player P_1 is the encoder, such that for all $\mathcal{Q}_1 \in \mathbb{Q}_1$ there exists a distribution,

$$\widetilde{\mathcal{Q}_1} \in \Delta(\mathcal{U}_2 \times \mathcal{U}_3 \times \mathcal{A}_1 \times \ldots \mathcal{A}_3 \times \mathcal{S}_1 \times \ldots \mathcal{S}_4)$$

satisfying the two following conditions:

- the conditions on the marginals:

$$\begin{aligned} \sum_{u,s} \widetilde{\mathcal{Q}_1}(u,a,s) \quad &= \quad \mathcal{Q}_1(a) \\ \widetilde{\mathcal{Q}_1}(s|u,a) \quad &= \quad T(s_2,s_3,s_4|a_1,a_2,a_3) \end{aligned}$$

- the information theoretical conditions:

$$\begin{aligned} H(A_2) \quad &\leq \quad I(U_2;S_2,A_2) \\ &- \quad \max(I(U_2;S_4), I(U_2;A_2,A_3)) \\ H(A_3) \quad &\leq \quad I(U_3;S_3,A_3) \\ &- \quad \max(I(U_3;S_4), I(U_3;A_2,A_3)) \\ H(A_2) \quad &+ \quad H(A_3) \leq I(U_2;S_2,A_2) \\ &+ \quad I(U_3;S_3,A_3) - I(U_2;U_3) \\ &- \quad \max(I(U_2,U_3;S_4), I(U_2,U_3;A_2,A_3)) \end{aligned}$$

Define in a similar way $\mathbb{Q}_2$ (resp. $\mathbb{Q}_3$), when player P_2 (resp. player P_3) is an encoder in the above channel model. Let $\mathbb{Q}_{123}$ denote the convex hull of the union of achievable distributions when one of the players is an encoder:

$$\mathbb{Q}_{123} = \text{co } [\mathbb{Q}_1 \cup \mathbb{Q}_2 \cup \mathbb{Q}_3 \cup X_{123}] \subset \Delta(\mathcal{A}_{123})$$

Theorem 8: Suppose that the channel transition T does not depend on the actions of the fourth player:

$$\begin{aligned} T(s_1,s_2,s_3,s_4|a_1,a_2,a_3,a_4) \quad &= \quad T(s_1,s_2,s_3,s_4|a_1,a_2,a_3), \\ &\qquad \forall a_k, s_k, \ k \in \mathcal{K} \end{aligned}$$

The uniform min-max level v_4^∞ of player P_4 for the repeated game with signals is upper bounded by the following quantity:

$$v_4^\infty \leq \min_{\mathcal{Q}\in\mathbb{Q}_{123}} \max_{a_4\in\mathcal{A}_4} \mathbb{E}_Q u_4(a_1,a_2,a_3,a_4) = \nu$$

D. Sketch of the proof of Theorem 8

We have proven that the coding scheme described in the previous section is optimal for the players in order to guarantee the value $\nu \in \mathbb{R}$. Face to the above strategy for players P_1, P_2 and P_3, every strategy τ_4 for player P_4, leads to a long-run expected utility below $\nu \in \mathbb{R}$. Suppose that the optimal distribution $Q^* \in \Delta(\mathcal{A}_{123})$ is a convex combination:

$$Q^* = \sum_{j=1}^{J} \alpha_j Q_j^* \in \mathbb{Q}_{123} \tag{49}$$

The play of players P_1, P_2 and P_3 is divided into J blocks of stages of length N_j where the players implement Q_j^*. Each block $\mathcal{N}_j$ of stages is divided into $I+1$ sub-block $\mathcal{N}_j^i$ where the encoding player communicate to the others, the sequence of actions they will play in the next sub-block. The recursive coding process is described in Fig. VI-D.

For each sub-block $i \in I$, the coding scheme consists of a concatenation of the Shannon's source coding scheme [5] and the channel coding scheme investigated here above. The joint source coding scheme is described in Fig. VI-D where $\mathcal{A}_k^i$ denotes the sequence of actions of player P_k during the sub-block of stages $\mathcal{N}_j^i$. The entropy constraints (49) in

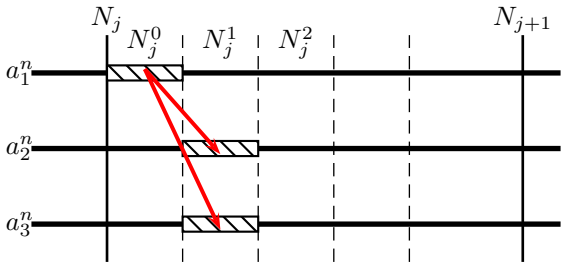

Fig. 5. During the sub-block N_j^0 player P_1 wants players P_2 and P_3 to play certain actions during the sub-block of stages N_j^1. It can be noticed that the knowledge of the sequence of future realizations of the channel state (non-causal side information) at the encoder is therefore fully justified from a game theoretical point of view.

the definition of $\mathbb{Q}_{123}$ insure that the sequence of actions of players can be sent over the channel and recovered with an arbitrary small error probability.

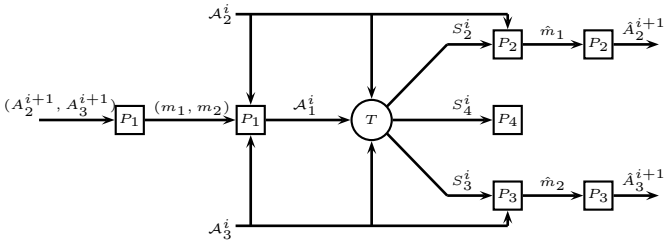

Fig. 6. The joint source channel coding scheme for transmitting during the sub-block of stages $\mathcal{N}_j^i$ the actions of the sub-block of stages $\mathcal{N}_j^{i+1}$.

Our coding scheme guarantees that the expectation of the empirical distribution of plays $\mathbb{E}[\bar{Q}]$ converges to the optimal distribution Q^*. Second, the coding scheme guarantees that the distribution over the signals s_4^n of player P_4 prevents her to guess the future sequence of correlated actions of the players P_1, P_2 and P_3.

VII. Conclusion

This paper investigates a generalization of the wiretap channel with two receivers and one eavesdropper where the channel transition depends on states known non-causally and perfectly at the encoder and partially known at both receivers. The main theorem of the paper provides an achievable rate region. Applying the theorem to the Gaussian case allows one to make several interesting observations. In particular, two scenarios have been studied. In the first scenario, we have shown that, contrarily to [4] and related works, having side information at the decoder in addition to having it at the encoder is useful when security constraints come into play. Whereas this result has been proved for the Gaussian case, further works should be necessary to study the discrete case (e.g., by introducing more auxiliary variables to fully exploit the knowledge of the side information at the encoder). In the second scenario, it is shown that the presence of known perturbations (namely S_1 and S_2) can enhance the secrecy rates. In fact, if those perturbations are sufficiently strong, it is even possible to obtain the same rate region as if the eavesdropper were not present. Another type of interesting result is that we show how multiuser Shannon theory can be exploited for general games, opening a general methodology to derive communication-compatible game-theoretic such as min-max levels, feasible joint distributions or correlated strategies, etc. One the key observations made in this paper is that source-channel theorems might play an increasing role in games where inter-player communications is allowed.

References

[1] R. J. Aumann, M. Maschler, and R. E. Stearns. *Repeated Games with Incomplete Information*. The MIT Press, 1995.

[2] G. Bagherikaram, A.S. Motahari, and A. K. Khandani. Secure broadcasting : The secrecy rate region. In *Proc. 46th Annual Allerton Conference on Communication, Control, and Computing*, pages 834–841, Sept. 2008.

[3] Y. Chen and H. Vinck. Wiretap channel with side information. *IEEE Transactions on Information Theory*, 54(1):395–402, 2008.

[4] M. H. M. Costa. Writing on dirty paper. *IEEE Transactions on Information Theory*, 29:439–441, 1983.

[5] T.M. Cover and J.A. Thomas. Elements of information theory. *Wiley-Interscience*, 1991.

[6] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978.

[7] I. Csiszár and J. Körner. *Information Theory: Coding Theorems for Discrete Memoryless Systems*. 1981.

[8] A. A. El Gamal and E. van der Meulen. A proof of Marton's coding theorem for the discrete memoryless broadcast channel. *IEEE Transactions on Information Theory*, 27(1):120–122, Jan. 1981.

[9] D. P. Palomar G. Scutari and S. Barbarossa. The mimo iterative waterfilling algorithm. *IEEE Trans. Signal Process.*, 57(5):19171935, May. 2009.

[10] S. I. Gel'fand and M. S. Pinsker. Coding for channel with random parameters. *Problems of Control and Inform. Theory*, 9(1):19–31, 1980.

[11] O. Gossner and T. Tomala. Empirical distributions of beliefs under imperfect observation. *Mathematics of Operation Research*, 31(1):13–30, 2006.

[12] O. Gossner and T. Tomala. Secret correlation in repeated games with imperfect monitoring. *Mathematics of Operation Research*, 32(2):413–424, 2007.

[13] A. Khisti, A. Tchamkerten, and G.W. Wornell. Secure broadcasting over fading channels. *IEEE Transactions on Information Theory*, 54:2453–2469, 2008.

[14] S. Lasaulce, M. Debbah, and E. Altman. Methodologies for analyzing equilibria in wireless games. *IEEE Signal Processing Magazine, Special issue on Game Theory for Signal Processing*, Sep. 2009.

[15] K. Marton. A coding theorem for the discrete memoryless broadcast channel. *IEEE Transactions on Information Theory*, 25:306–311, Mar. 1979.

[16] J. Renault and T. Tomala. General properties of long-run supergames. *Dynamic Games and Applications*, 1(2):319–350, 2011.

[17] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 1948.

[18] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.

[19] Y. Steinberg and S. Shamai. Achievable rates for the broadcast channel with states known at the transmitter. In *Proc. International Symposium on Information Theory ISIT 2005*, pages 2184–2188, 4–9 Sept. 2005.

[20] G. Ginis W. Yu and J. M. Cioffi. Distributed multiuser power control for digital subscriber lines. *IEEE J. Sel. Areas Commun.*, 20(5):11051115, May. 2002.

[21] A. D. Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, 1975.